IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

DIGITAL REG OF TEXAS, LLC.,	§	
	§	
Plaintiff	§	
	§	
vs.	§	**CASE NO. 6:07 CV 467**
	§	**PATENT CASE**
LFP INTERNET GROUP, LLC, L.F.P., INC., MICROSOFT CORP., APPLE INC., PLAYBOY ENTERPRISES, INC., AUDIBLE, INC., SONY CORP. OF AMERICA, SONY CONNECT, INC., MACROVISION CORP., and BLOCKBUSTER INC.	§	
	§	
Defendants	§	

MEMORANDUM OPINION AND ORDER

This opinion construes the terms of U.S. Patent No. 6,389,541. Also before the Court are Audible's motion for summary judgment for invalidity of claim 2 for failure to comply with 35 U.S.C. § 112, ¶ 2 (Docket No. 236) and Sony's motion for summary judgment of invalidity based on indefiniteness and written description under 35 U.S.C. § 112 (Docket No. 237). Having considered the parties' written submissions and oral arguments, the Court **DENIES** Audible's and Sony's motions.

BACKGROUND

The '541 patent concerns the regulation of access to digital content such as text, video, and music that has been downloaded onto a client computer. The downloaded content is inaccessible until installation is authorized. The authorization, which is signified by a transmitted token received by the client computer, involves routing user information through a server to an authorization center.

Upon access authorization being granted, the authorization center sends an authorization signal back to the server. In response, the server sends a "token" to the client computer. Receipt of the token unlocks a unique coded key corresponding to the content to be installed on the client computer, which initiates an installation process for the content that makes the content accessible. The content is made accessible on only the particular client computer that receives the token.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In claim construction, courts examine the patent's intrinsic evidence to define the patented invention's scope. *See id.*; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id*. Other asserted or unasserted claims can also aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id*. Differences among the claim terms can also assist in understanding a term's meaning. *Id*. For example, when a

dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id*. at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id*. (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id*. (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id*. Also, the specification may resolve ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex, Inc.*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.'" *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "'less significant than the intrinsic record in determining the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (quoting

C.R. Bard, Inc., 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id*. at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id*. Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id*.

DISPUTED TERMS[1]

Preamble and **Order of steps in claim 1**

Whether the preamble is a limitation is not the real dispute on this issue. Defendants contend that the steps of claim 1, which are in the body of the claim, not the preamble, must logically be performed in the order they are listed. In its reply brief, Digital Reg argues that the steps are not limited to the order in which they are claimed.

"[A]lthough a method claim necessarily recites the steps of the method in a particular order, as a general rule the claim is not limited to performance of the steps in the order recited, unless the claim explicitly or implicitly requires a specific order." *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1345 (Fed. Cir. 2008) (citing *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342–43 (Fed. Cir. 2001)). However, "[t]he specification or prosecution history may also require a narrower, order-specific construction of a method claim in some cases." *Id*.

Claim 1, step 1 is "at a client, executing an access checking process to determine whether the client holds a pre-existing permission for a resource to access the digital content." The second step

[1] Appendix A contains the relevant claims with the disputed terms in bold.

is if the client does not hold a pre-existing permission for a resource to access the digital content, "requesting permission from an external source for the resource to access the digital content." Thus, step 2 logically must follow step 1. Step 3 is "receiving from the external source a token." This happens in response to "requesting permission from an external source" and so must follow step 2. Step 4 is "based on the received token, executing an installation process . . . ." Thus, step 4, which is based on the token received in step 3, must logically come after step 3.

Accordingly, the steps are limited to the order in which they are claimed. Digital Reg contends that because claim 1 uses the term "comprising" a method may utilize additional steps and still infringe the claim. While this is true, it does not change the conclusion that the steps that are claimed must be performed in the order in which they are claimed.

Token

Digital Reg contends "token" should be construed as "a file indicating whether access should be granted." Defendants contend "token" should be construed as "A file indicating whether the transaction has been approved; i.e. whether the object should be installed and access granted. The token is not stored on the client." Thus, the parties dispute whether a token indicates whether a transaction has been approved and whether a token must not be stored on the client.

To support their constructions, both sides point to the same part of the specification. The specification states:

> Upon receiving a message from the authorization center indicating either acceptance or rejection of the transaction, the payment server transmits a "token" back to the client computer. *The token is a file indicating whether the transaction has been approved, i.e. whether the objection should be installed and access granted.* If the token indicates approval, the token causes the client computer to execute the install process discussed previously, wherein, for example, a unique coded key corresponding to the object is installed at the client, along with the client machine identification code.

Col. 4:65–5:7 (emphasis indicating what the parties base their arguments on). The statement in the

specification that the token indicates approval of a transaction is made in the specific, illustrative context of the execution of a payment transaction. "Token," when read in the full scope of the disclosure, is not limited to a transaction. *See* col. 3:16–18 (describing that access is regulated through payment transactions or other authorization information); claim 13 ("the token received is based on a result of the *authorization* procedure"); claim 18 (limiting claim 13 to an authorization procedure that involves a payment transaction). The full disclosure requires only that "token" means "whether access should be granted."

Defendants also contend that the token may not be stored on the client. Defendants rely on the prosecution of claim 3. During prosecution, the applicant stated:

> The token is not stored, but rather is used as a permission at the client to store the unique key. The token, incapable of interception during transmission, exists on the client only long enough to generate the unique key. No longer existing, the token is incapable of being transferred to another client.

Defendants' Markman Brief (Docket No. 238), Ex. B at 134.[2] This was said in response to the examiner's rejection under 35 U.S.C. § 112, ¶ 1 of claim 3, that "the token on which selectively granting access [is based] is not transferable to another client." The examiner then stated, "The specification discloses writing the unique key, i.e. token, to a Windows registry file on page 16. However, the specification does not disclose a method to prevent transfer of the unique key to another client." Ex. B at 133–34.

Neither claim 1 nor the specification expressly require that the token not be stored. Claim 3 adds a further limitation about how the token is used rather than what the token is. During prosecution, the applicant was clarifying that the token is used at the client and exists at the client long enough for the generation of the unique key. The applicant was clarifying to the examiner that

[2] Exhibit B to Defendants' Markman Brief (Docket No. 238) is the prosecution history. For ease of reference, all cites to the prosecution history will be cited to as "Ex. B at ___."

the token and unique key were not the same thing. The token is necessarily stored on the client long enough to generate the unique key. Thus, this statement is not tantamount to a disclaimer that the token should be limited to not being stored. Claim 1 is non-specific and is not written to disclaim storage of the token in the client's registry.

Accordingly, the Court construes "token" as "a file indicating whether access should be granted."

Executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process

Defendants offer a construction for the entire term, but Digital Reg contends that only "a permission" and "a permission that is locked uniquely to the client" require construction.[3] Thus, the first dispute is whether the executing step should be construed as a whole or whether only portions of it should be construed. Digital Reg argues that Defendants' approach and lengthy construction do not simplify the meaning of the limitation to the jury and adds a number of limitations to the term that are not recited in the claim. Defendants contend that a piecemeal approach will not resolve the parties' disputes. The Court agrees that a piecemeal approach will not address all of the parties' disputes and will construe the term as a whole as well as construe the individual terms that Digital Reg contends require construction.

Defendants contend "executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process" should be construed as "Running an installation program that generates a permission, which permission is both (1) locked uniquely to the client and (2) may be located in memory by a later execution of the access checking process. This permission must be generated

[3] Initially Digital Reg also proposed a construction for "executing an installation process," but the parties have now agreed that this term should be given its plain and ordinary meaning.

locally, at that particular client, as opposed to occurring across a network or at a central computer. The term 'generates at the client a permission that is locked uniquely to the client' does not cover the storage of a permission or the recalculation of a permission, or any combination thereof, occurring at the client." Digital Reg contends that portions of Defendants' construction mirrors the claim language, but objects to Defendants' limitations that (1) the permission "may be located in memory," (2) that the permission "must be generated locally, at that particular client, as opposed to occurring across a network or at a central computer," and (3) "'generates at the client a permission that is locked uniquely to the client' does not cover the storage of a permission or the recalculation of permission, or any combination thereof, occurring at the client."

located in memory and *generated locally*

At the hearing, the parties resolved their disputes over the first two issues by agreeing to construe the term as "running an installation program that creates a permission locally, which permission is (1) locked uniquely to the client and (2) capable of being found locally by a later execution of the access checking process."

storage of a permission or recalculation of a permission

Defendants contend that "'generates at the client a permission that is locked uniquely to the client' does not cover the storage of a permission or the recalculation of a permission, or any combination therefore, occurring at the client." Defendants contend that during prosecution, the applicant distinguished the client-based operations of *Wolfe*, i.e. storage and recalculation, from the claimed generation of permission at the client.

The examiner's rejection and the arguments made to distinguish *Wolfe* did not implicate "client-side" activities, but only "server-side" activities. Therefore, specifying that the generation is done "locally" is sufficient, and Defendants' remaining language is not appropriate.

Accordingly, the Court construes "executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process" as "running an installation program that creates a permission locally, which permission is (1) locked uniquely to the client and (2) capable of being found locally by a later execution of the access checking process."

A permission

Digital Reg first contends that only "a permission" in "a permission that is locked uniquely to the client" requires construction, and "a permission" should be construed as "information which grants access." Defendants contend that the entire phrase, "a permission that is locked uniquely to the client" requires construction.

To support its construction, Digital Reg relies on claim 4, which states "wherein the permission comprises a unique coded key corresponding to the digital content." Digital Reg also cites to claims 21 and 26, which include a "permission key," as consistent with its proposed construction. Finally, Digital Reg cites to the specification, which states, "[e]very unique object has a unique coded key which acts as a key for accessing the object." Col. 8:58–61. This unique coded key acts as a key for accessing the object. Digital Reg contends this explanation of a unique coded key supports its construction of "a permission" as "information which grants access."

Defendants contend that "a permission" should not be construed outside the broader phrase of "a permission that is locked uniquely to the client." Defendants do however state that "permission" is synonymous with "unique coded key." Responsive Brief (Docket No. 238) at 23 ("the inventor used the term 'permission' as a synonym for the 'unique coded key'"). Defendants contend Digital Reg's proposed construction is unsupported by the specification or prosecution history and that Digital Reg does not explain how claim 4 supports its construction. Finally,

Defendants argue that "a permission" is used in different ways in claim 1, which raises issues of indefiniteness and written description that Digital Reg seeks to avoid by only construing "a permission" as it is used in the phrase "a permission that is locked uniquely to the client." Sony moves for summary judgment based on indefiniteness and lack of written description on these grounds. *See* Docket No. 237.

A claim is invalid under 35 U.S.C. § 112, ¶ 2 if it fails to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. The party seeking to invalidate a claim under 35 U.S.C. § 112, ¶ 2 as indefinite must show by clear and convincing evidence that one skilled in the art would not understand the scope of the claim when read in light of the specification. *Intellectual Prop. Dev., Inc. v. UA-Columbia Cablevision of Westchester, Inc.*, 336 F.3d 1308, 1319 (Fed. Cir. 2003).

"The definiteness requirement of § 112, ¶ 2 'focuses on whether the claims, as interpreted in view of the written description, adequately perform their function of notifying the public of the [scope of the] patentee's right to exclude.'" *Honeywell Int'l, Inc. v. Int'l Trade Comm'n*, 341 F.3d 1332, 1338 (Fed. Cir. 2003) (quoting *S3 Inc. v. nVIDIA Corp.*, 259 F.3d 1364, 1371-72 (Fed.Cir.2001)). "It requires that the claims be amenable to construction, however difficult that task may be. Because a claim is presumed valid, a claim is indefinite only if the claim is insolubly ambiguous, and no narrowing construction can properly be adopted." *Id*. at 1338–39 (citations omitted).

"[T]he purpose of the written description requirement is to 'ensure that the scope of the right to exclude, as set forth in the claims, does not overreach the scope of the inventor's contribution to the field of art as described in the patent specification.'" *ICU Med., Inc. v. Alaris Med. Sys., Inc*., 558 F.3d 1368, 1376 (Fed. Cir. 2009) (quoting *Univ. Rochester v. G.D. Searle & Co.*, 358 F.3d 916,

920 (Fed. Cir. 2004)). The written description requirement protects the quid pro quo between inventors and the public, where the public receives meaningful disclosure of the invention in exchange for being prohibited from practicing the invention for a limited time period. *Id*. at 1377. To comply with 35 U.S.C. § 112's written description requirement, the applicant must "'convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention,'" which is whatever is now claimed. *Id*. (quoting *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991)). The description does not need to "recite the claimed invention in haec verba but must do more than merely disclose that which would render the claimed invention obvious." *Id*.

"A permission" satisfies § 112's written description requirement. Defendants admit that the term "permission" is generic to the disclosed species of a "unique coded key." Claims commonly use a generic term when only a species is disclosed. One example is a disclosure of a novel dwelling of frame construction wherein the illustrated embodiment only describes that nails are used to connect the framing materials together. A nail is one species of fastener and a screw is another. A claim to the dwelling structure permissibly recites a "fastener," which is a generic term to both a nail and a screw. Similarly, the generic term "permission" is properly used in view of the disclosure of only a single species, a "unique coded key." *See Ethicon Endo-Surgery, Inc. v. U.S. Surgical Corp.*, 93 F.3d 1572, 1582 n.7 (Fed. Cir. 1996) (citing *In re Vickers*, 141 F.2d 522, 525 (C.C.P.A. 1944) ("an applicant . . . is generally allowed claims, when the art permits, which cover more than the specific embodiment shown")); *In re Rasmussen*, 650 F.2d 1212, 1214 (C.C.P.A. 1981) (disclosure of a single method of adheringly applying one layer to another was sufficient to support a generic claim to "adheringly applying" because one skilled in the art reading the specification would understand that it is unimportant how the layers are adhered, so long as they are adhered).

Additionally, the term "permission" when read in the context of its usage is clear. "A permission," as used throughout the claim language, is not indefinite or insolubly ambiguous. When the same term appears in different portions of the claims, courts presume that it should be given the same meaning "unless it is clear from the specification and the prosecution history that the terms have different meanings at different portions of the claims." *Fin Control Sys. Pty, Ltd. v. OAM, Inc.*, 265 F.3d 1311, 1318 (Fed. Cir. 2001). Step 1 uses the phrase "whether the client holds a pre-existing permission." Step 2 claims "requesting permission," and step 4 claims "an installation process that generates at the client a permission." Both sides agree that "a permission" is used differently in steps 1 and 4 than in step 2. This is clear from the claim language itself and does not render the term insolubly ambiguous. The same term may be interpreted differently at different portions of the claim when it is clear from the specification that the term has different meanings. *See id.* The specification includes the claims; and, thus, the case law supports the conclusion that the term is not indefinite. Accordingly, the Court construes "a permission" as "information which grants access." The Court **DENIES** Sony's motion for summary judgment.

A permission that is locked uniquely to the client

Digital Reg contends that this phrase does not require construction or alternatively should be construed as "information which grants access, said access specific to the client." Defendants contend that "a permission that is locked uniquely to the client" should be construed as "a unique coded key that is stored at the client along with a machine identification code of the client. The permission is separate and distinct from the token."

Digital Reg contends Defendants' construction is improper because it imports limitations from the specification and dependent claims. Specifically, Digital Reg contends that Defendants' attempt to limit the claims to the preferred embodiment and subject of claim 4 of "a unique coded

key" is improper. Relying on a preferred embodiment described at column 10, lines 62 to column 11, line 3, Digital Reg also contends that incorporating the machine identification code of the client within the permission is improper because these are two different bits of information. Finally, Digital Reg contends that Defendants' limitation that the permission is "separate and distinct" from the token is incorrect because the token and permission work in tandem—when the token is received, an installation process is executed, and a permission is generated. Whether the permission is attached to the object, token, or nothing is irrelevant to claim 1's method.

Defendants support their limitation of "a unique coded key" by arguing that support for the step of "executing an access checking process to determine whether the client holds a pre-existing permission" is found in Figure 5, which the patent refers to as "a flow chart illustrating a check coded key, or 'access check,' function." *See* col. 6:61–62. Defendants also contend the claimed permission is "locked" to the client and whenever the specification discusses "locking"something to a client, it refers to storing a unique coded key along with a machine ID of the client. *See* col. 3:48–60; 8:58–9:9; 10:67–11:3. As previously stated, Defendants contend "permission" is used in the specification and prosecution history synonymously with a "unique coded key." *See* Ex. B at 138; col. 8:58–61. Defendants contend that the claims require the permission is separate and distinct from the token because the claims separately recite a "token" and "permission" and a dependancy between them (that the permission is generated based on the token). *See* claim 1 ("based on the received token, executing an installation process that generates at the client a permission that is locked uniquely to the client . . . ."); *see also* col. 10:59–11:9.

For the reasons discussed above, "permission" is not limited to a "unique coded key." Defendants' construction limits the term to the details of the disclosed embodiment and narrows the term to include the machine ID, which is not part of the information that grants access to the digital

content. Accordingly, the Court does not adopt Defendants' construction.

Digital Reg's construction is correct as to "information which grants access" but "said access specific to the client" does not properly take into account the portion of the claim term that states "that is locked uniquely to the client." The specification indicates that the permission (e.g., the coded key) is locked to the client in the sense that key cannot be moved to another machine along with the object. *See* col. 11:2–7. Thus, when the key is locked to the client, it is confined from moving to another machine. It is described that the key is confined by associating the client machine ID with the key. Accordingly, the Court construes "a permission that is locked uniquely to the client" as "information which grants access, said access being confined to the client."

An authorization procedure

Digital Reg argues that this term does not require construction or alternatively should be construed as "a process which determines whether access should be granted." Defendants contend the term should be construed as "a process that determines whether a transaction is accepted or rejected."

Digital Reg argues that Defendants' construction improperly imports limitations from the specification into the claims. Specifically, Digital Reg objects to Defendants' use of the word "transaction," which Digital Reg contends is only used in the specification to describe situations where payment is required. *See* Abstract ("The payment authorization center approves or rejects the payment transaction, and bills the corresponding account. The authorization center then transmits an authorization signal to the payment server computer indicating whether the transaction was approved."). Digital Reg contends that it is clear from the specification and the claims that either payment or use information can be provided to gain access to content. *See* col. 4:13–16; claim 20.

Defendants contend that the term's ordinary meaning is a procedure that will either approve

or reject the client's requests to access the client, i.e., will authorize the request. Defendants contend that in the step described in claim 13, the external source reviews the information provided by the client, e.g., use and payment information, to determine whether the external source should provide a token to the client that will allow the client to execute an installation process to generate the unique permission for the digital content. *See* col. 4:30-46. Defendants argue that the specification describes the authorization procedure as occurring at an external source and that the purpose of the procedure is to determine whether the external source should approve or deny a client's request for permission to receive a resource to access the digital content.

As argued by Digital Reg, and as discussed with regard to "token," limiting the term to "transaction[s]" is overly narrow. Defendants' construction is also overly limiting in that it specifies an act of either acceptance or rejection. "Authorization" carries a broader meaning consistent with Digital Reg's proposal of "access should be granted." Claim 13, in view of its dependence on claim 1, connotes granting access to digital content. Inclusion of "acceptance or rejection" is not consistent with the language "based on a result of the authorization procedure" in claim 13. Accordingly, the Court construes "an authorization procedure" as "process which determines whether access should be granted."

Use information

Digital Reg contends this term does not require construction or alternatively should be construed as "information which a content producer or supplier wishes to consider in regulating access to the digital content." Defendants contend the term means "data used to control, for example, circulation materials such as industry and trade publications, which require the recipient to provide employment data in order to have a 'no charge' edition of the publication."

To support its proposed construction, Digital Reg cites to the specification, which states

"Alternatively or in addition to payment information, use information may be required, such as employment-related data, educational information, family information, or any other information which a content producer or supplier wishes to consider in regulating access to the object." *See* col. 4:22–26. Digital Reg contends Defendants' construction improperly relies on examples in the specification that describe a preferred embodiment.

Defendants contend that the passage from the specification that Digital Reg relies on is not intended to define "use information" but merely describes the type of use information that may be required. *See* col. 4:22–26. Defendants argue that the specification explicitly defines "use information": "Use information is data used to control, for example, circulation materials such as industry and trade publications, which require the recipient to provide employment data in order to have a 'no charge' edition of the publication." *See* col. 9:32–36.

Thus, both parties contend the specification expressly defines the term, but they disagree on which portion of the specification is defining and which is exemplary. Column 4, lines 22-26 give a generic description of "use information," which serves a definition. Column 9, lines 32–36 is a subset of what is set forth in column 4. Accordingly, the Court construes "use information" as "information which a content producer or supplier wishes to consider in regulating access to the digital content."

AUDIBLE'S MOTION FOR SUMMARY JUDGMENT

Audible argues that claim 2 is indefinite under 35 U.S.C. § 112 because during prosecution claim 1 was amended to remove the limitation "selectively granting the resource access to the digital content" but "selectively granting the resource access" was not removed from claim 2. Audible contends that "selectively granting the resource access" in claim 2 lacks antecedent basis and it is unclear whether "selectively granting the resource access" in claim 2 relates to the pre-permission

check that occurs at the client, relates to the generation at the client of the permission that it locked uniquely to the client, whether it is a result of a combination of steps that require transaction with an external source, or whether it is a separate and completely new step not contained in claim 1.

Claims 1 and 2 state:

> 1. A computer-implemented method of regulating access to digital content, the method comprising:
>
> at a client, executing an access checking process to determine whether the client holds a pre-existing permission for a resource to access the digital content;
>
> if not, requesting permission from an external source for the resource to access the digital content;
>
> receiving from the external source a token; and
>
> based on the received token, executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process.
>
> 2. The method of claim 1, wherein requesting the permission, receiving the token, and selectively granting the resource access are performed on the client.

Claim 2 incorporates all of the limitations of claim 1, with the further limitations that requesting the permission, receiving the token, and selectively granting the resource access are performed on the client. While requesting the permission and receiving the token both refer to steps recited in claim 1, selectively granting the resource access does not. One of skill in the art would recognize that this is a separate and additional step that is not contained in claim 1. As a separate and additional step, Audible's contention that "selectively granting the resource access" lacks antecedent basis is without merit. Although no party has asked the Court to construe the term, the term does not require construction because it is used in its plain and ordinary meaning. Accordingly, the Court **DENIES** Audible's motion.

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. The claims with the disputed terms in bold are set forth in Appendix A. For ease

of reference, the Court's claim interpretations are set forth in Appendix B.

So ORDERED and SIGNED this 13th day of July, 2009.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPENDIX A

1. A computer-implemented method of regulating access to digital content, the method comprising:
    at a client, executing an access checking process to determine whether the client holds a pre-existing permission for a resource to access the digital content;
    if not, requesting permission from an external source for the resource to access the digital content;
    receiving from the external source a **token**; and
    based on the received token, **executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process.**

2. The method of claim 1, wherein requesting the permission, receiving the token, and selectively granting the resource access are performed on the client.

13. The method of claim 1, wherein **requesting the permission** from the external source initiates **an authorization procedure**, and the token received is based on a result of the authorization procedure.

20. The method of claim 13, wherein the authorization procedure comprises:
    processing **use information** received from a client;
    searching the use information for a predefined parameter;
    and
    transmitting the token to the client based on a result of the search.

APPENDIX B

Disputed term	**Court's construction**
token	a file indicating whether access should be granted
executing an installation process that generates at the client a permission that is locked uniquely to the client and that may be found by a later execution of the access checking process	running an installation program that creates a permission locally, which permission is (1) locked uniquely to the client and (2) capable of being found locally by a later execution of the access checking process
a permission	information which grants access
a permission that is locked uniquely to the client	information which grants access, said access being confined to the client
an authorization procedure	process which determines whether access should be granted
use information	information which a content producer or supplier wishes to consider in regulating access to the digital content